National Infrastructure Protection Center
NIPC Daily Open Source Report
for 27 January 2003

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here
www.whitehouse.gov/homeland

Daily Overview

- Reuters reports the unusually high natural gas prices are putting a squeeze on power plant operators who are finding they can make more money selling the fuel to the market than burning it to generate electricity. (See item 5)
- The "Slammer" worm causes disruptions to banking and airline operations in North America. (See item 9)
- UPI reports experts say the massive Internet outage that swept across Asia and slowed down service in the United States and northern Europe was caused by a so−called "Slammer" message worm that could easily have been avoided had system operators downloaded free repair software. (See item 21)
- The NIPC has released Advisory 03−001: "Worm Targets SQL Vulnerability." (See item 22)
- The Kansas City Channel reports that University of Kansas officials discovered Wednesday that a computer hacker had downloaded personal information gathered on 1,450 of its international students. (See item 23)
- Wired reports Sprint DSL customers are at risk of having their e−mail addresses and passwords stolen −− even when their computers are powered off −− due to weak security controls on their DSL modems. (See item 24)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *January 26, Associated Press* — **Crude oil spill in Great Lake tributary. A pipeline carrying crude oil ruptured, dumping nearly 19,000 gallons onto the frozen Nemadji River, a tributary of Lake Superior. At least 100,000 gallons spilled at Enbridge Energy Terminal, about two miles from the lake, but most of it was contained within the terminal's ditches and retention ponds, company officials said.** The pipeline is about half a mile from the terminal. The leak happened Friday night, apparently during delivery from the pipeline to a storage tank, said Mark Sitek, regional general manager for Houston−based Enbridge Energy. **Cleanup of the ice−covered river is expected to take a few days, Sitek said. Cleanup of the terminal could take as long as several weeks.** The Wisconsin Department of Natural Resources is monitoring the effort. Enbridge had a smaller oil spill in 2000, but that leak was contained within the terminal.
Source: http://www.cnn.com/2003/US/Midwest/01/26/superior.oil.ap/

2. *January 23, BBC Monitoring South Asia* — **Pakistan daily reports second attack on gas pipeline . Another gas pipeline in the Sui gas field of Baluchistan was blasted in Sui by unknown armed men on Wednesday (January 22) afternoon, partially cutting off the gas supply to some areas of Sindh and Baluchistan.** Some unknown terrorists set some explosive under pipeline No "26 Wheel" and blasted it. This caused leakage of gas and suspension of gas supply to various cities of Sindh and Baluchistan. However, the leakage was controlled by the Sui gas field authorities. **This was the second attack in less than 24 hours on the pipeline. On late Tuesday, two main pipelines were blown up in a rocket attack.** Because of the blasts, gas supply had already been partially cut off to the Punjab and the North West Frontier Province [NWFP]. Earlier, a team of technical staff of Sui Northern Gas Pipeline Limited (SNGPL) arrived Rajanpur to repair the damaged gas pipeline. The blast not only damaged the pipeline but also caused a huge fire and supply of gas to the Punjab and the NWFP was suspended. Repair work is under way. The incident occurred as Mazari and Bugti tribes, due to old enmity, had indulged in exchange of firing rockets at each other and some of the rockets hit the pipeline causing its destruction. **Sources told The News that the gas wasted in the fire caused loss of billions of rupees to the government. It may be recalled that it was the fourth time that the main gas pipeline from Sui to the Punjab and onwards to the NWFP was destroyed.**
Source: http://www.energycentral.com/sections/gasnews/gn_article.cfm ?id=3590613

3. *January 23, Reuters* — **Dominion sees North Anna nuke in service by end of January.** Dominion Resources Inc.'s Dominion Energy said Thursday it **replaced the reactor vessel head on its 921 megawatt North Anna 2 nuclear unit in Virginia and expects to return the unit to service by the end of January.** The company also said in a statement it will replace reactor heads at the adjacent 921 MW North Anna 1 nuclear unit and its 800 MW Surry 1 nuclear unit in Virginia this spring as well as the 800 MW Surry 2 unit in the autumn. **The North Anna 2 unit, located in Mineral, Virginia, has been shut since early September, when operators found minor indications of leakage in the welds that attach control rod guides and instrument tubes to the vessel head. Reactor vessel head problems have come under scrutiny in the past year following the discovery of cracks in the lid capping a reactor at FirstEnergy Corp.'s Davis Besse nuclear plant in Ohio.** Repair bills for the U.S. nuclear power industry's pressurized water reactors similar in design to Davis Besse and North

Anna are likely to top $1 billion, according to industry estimates. Sixty−nine out of 103 working nuclear reactors in the U.S. are pressurized water reactors.
Source: http://www.energycentral.com/sections/newsroom/nr_article.cf m?id=3590479

4. *January 23, Associated Press* — **Northwest wind farm becomes largest producer. A wind farm along the Oregon−Washington border generated more electricity than any other wind power producer in the world last year, industry officials said Thursday. The Stateline Wind Project increased its megawatts from 263 to 300, pushing it ahead of the 278−megawatt King Mountain Wind Ranch in Texas, said Christine Real de Azua, spokesperson for the American Wind Energy Association.** Overall, she said, wind farm installations increased about 10 percent in the United States in 2002. Stateline uses turbines to catch wind off the Columbia River gorge and generates enough power to light 70,000 homes. The farm and the Texas operation are owned by FPL Energy, a subsidiary of Florida Power &Light Co. and the nation's largest wind energy producer.
Source: http://hsweb01.screamingmedia.com/PMA/pma_newsarticle1_natio nal.htm?SMDOCID=apdigital_2003_01_23_ap.online.regional.us_D 7OO63IO0_news_ap_org.anpaa>

5. *January 23, Reuters* — **Soaring natural gas prices idle U.S. power plants . High natural gas prices are putting a squeeze on power plant operators who are finding they can make more money selling the fuel to the market than burning it to generate electricity.** While heating demand typically pushes up East Coast gas prices during the winter months, this year's prohibitively high prices have been given an extra boost by a severe cold snap this month and widespread power plant outages in the region. **The price of natural gas has crept so high, in fact, that AES Corp. has been paid to keep its 705 megawatt (MW) Ironwood plant in Pennsylvania mostly idle since October so the fuel could be sold elsewhere.** A similar situation exists at AES' 832 MW Red Oak plant in New Jersey, which has been mostly idle for months due, in part, to high prices for natural gas, which is used to generate about 15 percent of the Northeast's electricity. Williams Energy Marketing, which has a 20−year power purchase agreement with AES's Ironwood and Red Oak plants, pays the Arlington, Virginia−based power provider each month for access to the plants regardless of whether they generate any electricity. Under the power purchase or "tolling" agreement, Williams Energy Marketing, a unit of Williams Cos Inc. of Tulsa, Oklahoma, delivers natural gas to the plants and takes back electricity. Williams then sells the power to its customers or into the Pennsylvania−New Jersey−Maryland market. Energy industry analysts have issued recent warnings that natural gas prices could hit $8 per million British thermal units (mmBtu) before the end of the winter, roughly three times what they fetched a year ago, if East Coast temperatures remain below normal much longer. **Natural gas is skyrocketing because supplies are shrinking and drilling activity has not yet caught up with the rising demand linked to the cold snap. Power plant operators typically do not discuss operations at their facilities, but energy traders generally agree gas−fired units have been dropped from the grid in favor of the usually bigger and cheaper coal−fired and nuclear units.** Until the demand for power eases or natural gas supplies increase, other plant operators may decide to idle their gas plants rather than waste the fuel by burning it.
Source: http://www.energycentral.com/sections/newsroom/nr_article.cf m?id=3590499

[Return to top]

Chemical Sector

6. *January 24, Umatilla Chemical Depot News* — **Forum looks at 'what ifs' in a depot disaster . A major explosion at the Umatilla Chemical Depot could devastate the area's economy and prompt emergency managers in Washington and Oregon to ask their governors for a disaster declaration. And such an accident involving chemical weapons agents also would likely create an immediate embargo on farm products, about 80 officials attending a daylong forum at Pendleton's Convention Center were told Thursday.** "We're not going to be able to sell anything out of Washington. It's going to affect our wineries, our orchards, our livestock and our transportation systems," said Rick Garza, Benton County Emergency Services manager. Determining who would be liable for damages was part of the session involving officials from Benton, Umatilla and Morrow counties, the Federal Emergency Management Agency, the Army, Environmental Protection Agency, Chemical Stockpile Emergency Preparedness Program, Oregon Department of Environmental Quality and Washington and Oregon Emergency Management and Health departments. **The economic damage could be immense, even if no nerve agent was released, said Tom Groat, Umatilla County emergency planner. Oregon health officials said the Army's capabilities present a problem. The difference between what's deadly and what's harmful can be difficult to assess, the state officials noted: a whiff of sarin might kill, but how little on an apple or grape is harmful?** FEMA plans to focus only on people's immediate needs, such as shelter and food. A chemical release would likely be more than just life−threatening, said Casey Beard, Morrow County emergency manager. **"People aren't going to be able to sell their homes and the real estate market will fall through the vent. Even if the plume were to affect only a small crop, we won't be able to ship any crops to any market.** And people aren't going to believe what we tell them because we've told them all along such an incident would never happen," Beard said.
   Source: http://www.umatilladepotnews.com/2003/0124.html

[Return to top]

Defense Industrial Base Sector

7. *January 24, New York Times* — **Plot to poison food of British troops is suspected.** Islamic militants arrested in Britain this month may have been plotting to lace the food supply on at least one British military base with the poison ricin, according to American government officials. The revelations raised concerns in Britain and the United States about the security of allied forces as war preparations continue. **American officials said they had received intelligence reports showing that the British authorities suspect that a group of militants arrested there in a series of raids may have been trying to gain access to the food supply on at least one military base in the United Kingdom. British officials found traces of ricin in a London apartment where the first arrests were made in the case.** "It's a very live theory," said one American law enforcement official familiar with the information from the British. **American officials said the reports showed that one of the suspects worked for a food preparation company and had been in contact with individuals who worked on at least one British military base. The United States officials said they did not know the identity of the suspect. They said they also did not know which British military base or**

bases might have been targets of the plot. Officials cautioned that the assessment is a working theory among British investigators, and that conclusive evidence had not yet been obtained. "There are some investigators who believe the ricin was being developed to poison British troops," an American official said. "But we still have found no direct evidence between the ricin discovery and that kind of plot." A spokesman for the British Home Office declined to comment on the reports.
Source: http://www.nytimes.com/2003/01/24/international/europe/24TER R.html

8. *January 24, New York Times* — **Pentagon's sturdy design saved lives, engineers find.** A "forest of columns" designed to support the Pentagon when it was built 60 years ago saved thousands of people who would otherwise have died when terrorists attacked it with a hijacked airliner on Sept. 11, 2001, an expert panel said in a report released today. **The study, sponsored by the American Society of Civil Engineers, said the sturdiness of the building and the closely spaced columns of reinforced concrete greatly limited the damage from the crash.** A team of six prominent structural engineers took seven months reviewing damage done by the attack to find out how better to protect existing and future buildings from similar assaults. The panel reviewed the original plans for the Pentagon, studied renovations that were under way at the time of the attack and analyzed aircraft data and eyewitness accounts. **"Based on analysis of this data, the team concluded that the Pentagon's resilient structural system, designed some 60 years ago, clearly mitigated the casualties and damage that resulted from the impact and fire," Paul F. Mlakar, the team leader, said at a Pentagon news conference. Dr. Mlakar, a technical director with the Army Corps of Engineers, credited the steel−reinforced columns, spaced about 20 feet apart, and the slab floors supported by a crisscross beam−and−girder system that helped spread excess loads from collapsed supports.** By contrast, the World Trade Center, where nearly 3,000 people died on Sept. 11, had open floors with few columns, and walls made of glass and lightweight steel.
Source: http://www.nytimes.com/2003/01/24/national/24PENT.html

[Return to top]

Banking and Finance Sector

9. *January 27, Washington Post* — **"Slammer" worm disrupts some banking and airline operations in operations in North America.** An Internet worm unleashed on Saturday impaired key systems in the U.S. government and private sector, delaying operations at one major airline and several media organizations, and knocking banks' cash machines offline. Bank of America Corp. said Saturday that most of its 13,000 automatic teller machines could not process customer transactions for part of the day because of the bug. Other banks also struggled this weekend with the effects of the worm, said Suzanne Gorman, chairman of the Financial Services Information Sharing and Analysis Center, which represents some of the nation's largest financial services companies. The worm caused flight delays and cancellations for Houston−based Continental Airlines after it overwhelmed the company's online ticketing systems and electronic kiosks that travelers use to check in, said company spokesman Jeff Awalt.
Source: http://www.washingtonpost.com/wp−dyn/articles/A46928−2003Jan 26.html

[Return to top]

Transportation Sector

10. *January 27,* — **See "Slammer" worm article in Banking and Finance Section.**
Source:

11. *January 24, Washington Post* — **U.S. weighs air security upgrades. Conceding that their airport bomb−sniffing machines have failed to work as well as hoped, two companies are asking the federal government to spend millions on new technology that would correct the defects.** The companies are working furiously to develop by next year technology that would enable 1,100 explosives−detection machines to scan checked luggage for bombs with improved accuracy. **The additional component would cost $100,000 to $200,000 per machine, adding up to $200 million to the $1.1 billion the government has already spent on the machines**, which cost $1 million apiece. The Transportation Security Administration, the agency in charge of airport security, said it was willing to consider new technology but has not committed to any further purchases. Chief executives of the firms acknowledged that the performance of their minivan−size machines needed to improve. **In a report to Congress in May, the TSA said the scanning devices typically produce false alarms 30 percent of the time, requiring security screeners to open suspect bags and search them by hand.** Since then, the agency has worked to improve performance; it now says that in a pilot project false alarms have been reduced to 15 percent. **Kenneth M. Mead, the Transportation Department's inspector general, said Thursday that the machines are one of his highest concerns about airport security.** "DOT knew they needed to do something about the alarm rates," he said, and **he encouraged the TSA to invest more money in research and development of other technologies.** "It's still an issue."
Source: http://www.washingtonpost.com/wp−dyn/articles/A35260−2003Jan 23.html

12. *January 23, U.S. Department of Transportation* — **DOT and American Public Transit Association form partnership to protect public transportation infrastructure. U.S. Transportation Secretary Norman Y. Mineta and American Public Transportation Association (APTA) President William W. Millar announced Thursday the formation of a new partnership to help protect the nation's public transportation infrastructure from terrorist and other attacks.** Secretary Mineta, APTA President William W. Millar, and Federal Transit Administrator (FTA) Jennifer L. Dorn pledged to work closely together to identify vulnerabilities, share threat information, and develop a joint plan to protect the nation's public transportation systems from attack. In early 2002, FTA began conducting security readiness assessments of the largest, highest−risk transit agencies. It was quickly concluded that transit systems need timely and transit−specific threat information and intelligence analysis. **In accepting the role of sector coordinator for the public transportation sector, Millar will act as the primary transit sector point of contact on transit−focused infrastructure protection issues, and will work closely with Secretary Mineta's sector liaison official, Rear Adm. Stephen Rochon, who is the director of the Secretary's Office of Intelligence and Security.** The department and APTA will sponsor a series of workshops that will help raise awareness of both physical and information−based threats and vulnerabilities to the nation's public transportation industry, and begin to develop strategies to address those threats. **APTA will establish a public transportation Information Sharing and Analysis Center (ISAC) where industry members can share security information, especially about evolving**

terrorist threats or ongoing information system attacks. FTA will provide the initial funding for the first two years of the ISAC and will continue as a member. The ISAC will work closely with ISACs established for other critical sectors, such as banking and finance and telecommunications, as well as with the National Infrastructure Protection Center.
Source: http://www.dot.gov/affairs/dot00803.htm

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

Nothing to report.
[Return to top]

Food Sector

13. *January 24, Associated Press* — **Bush to request $81 million more for food safety, official says. President Bush will seek an 11 percent increase in the U.S. Department of Agriculture's (USDA) 2004 food safety budget to strengthen protections against harmful bacteria in food and increase security at laboratories, officials said yesterday.** Agriculture Secretary Ann M. Veneman said that Bush will recommend $797 million in the budget he will send to Congress next month. That's $81 million more than in the 2002 budget, and an increase of $100 million, or 14 percent, over 2001. The 2003 budget proposal has yet to be approved by Congress. **Bush's recommendation "will further the USDA's efforts to protect consumers and the U.S. agricultural sector against threats, both intentional and unintentional," Veneman said yesterday.** USDA inspectors will focus on testing meat and poultry more frequently for bacteria such as listeria and E. coli, she said. Citing food−poisoning outbreaks that killed nine people last year, Veneman said, "Our goal is to reduce and eventually eliminate the need for recalls." **In addition to improving food safety protections, the proposed budget will include $70 million to increase security to guard against bioterrorism and the spread of pathogens, particularly at USDA laboratories where animal diseases, plant pests, and vaccines are studied. It also would be spent on improving monitoring.**
Source: http://www.boston.com/dailyglobe2/024/nation/Bush_to_request_81m_more_for_food_safety_official_says+.shtml

14. *January 24, Associated Press* — **Nebraska Beef, Ltd. reaches agreement, stays open. A meatpacker accused of unsanitary conditions reached an agreement Friday with the federal government that will prevent the business from being temporarily shut down. Nebraska Beef Ltd., which slaughters more than 2,000 cattle a day at its Omaha plant, had challenged a Jan. 14 attempt by the U.S. Department of Agriculture (USDA) to remove its inspectors, who must be present at slaughtering and processing operations.** A judge's order had blocked the move. A hearing on the issue had been scheduled for Thursday,

but it was postponed until Friday so the two sides could work out a settlement. The deal was reached as the hearing was set to start Friday. The details of the settlement were not immediately available. **In previous court papers, William C. Smith, a deputy administrator for the U.S. Department of Agriculture's Food Safety and Inspection Service, had argued that Nebraska Beef has a history of serious unsanitary conditions and inadequate food safety systems that have led to meat contamination.** Smith wrote that a shutdown was "necessary to protect the public health." Nebraska Beef argued it has responded sufficiently to USDA concerns, and it claimed in court documents that it has been subjected to scrutiny and penalties that were not assessed at other packing plants.
Source: http://www.omaha.com/index.php?u_np=02483

15. *January 24, Associated Press* — **Iowa packer ruling has implications in South Dakota. South Dakota officials are reviewing their past attempts to control corporate feedlots after a federal judge's ruling that Iowa's state ban on livestock ownership by meatpackers is unconstitutional. On Wednesday, U.S. District Judge Robert Pratt in Des Moines, Iowa, upheld a claim by Smithfield Foods Inc. that Iowa's ban on packer ownership of livestock was an unconstitutional infringement on interstate commerce.** Smithfield is the parent company of the John Morrell &Co. meatpacking plant in Sioux Falls, South Dakota. **South Dakota's laws do not ban interstate commerce, said Agriculture Secretary Larry Gabriel. But the Family Farm Act, which was adopted in 1974, restricts certain forms of ownership of land and buildings.** "Some people have been under the impression that it flirts with being unconstitutional, but I'm not a judge or a lawyer," Gabriel said Thursday. The state did try to control corporate livestock operations in 1998 with constitutional Amendment E. But a judge threw the measure out. The substitute, Amendment A, was rejected by state voters last June. **Imposing controls on the industry is tricky, Gabriel said. "I've never felt that corporations that are in the meatpacking business should be able to own livestock for a certain number of days before slaughter," said Gabriel, who is also a rancher. "But there is a downside: We have to be very careful here that we don't become such an advocate of the livestock industry that we kill the packers," Gabriel said.** "We need each other as a whole industry." Without a thought−out plan to restrict corporate farming, lawmakers could disrupt the feed−cattle market, too, he said. Some corporations buy a significant number of feeder cattle from auctions on certain days.
Source: http://www.aberdeennews.com/mld/aberdeennews/news/5023650.ht m

[Return to top]

Water Sector

16. *January 24, Water Tech Online* — **Stormwater regulations in California need to be overturned, group says. A coalition of 45 cities has filed a lawsuit to overturn California stormwater regulations that it feels could cost taxpayers billions of dollars and cause the loss of tens of thousands of jobs throughout Southern California.** The Coalition for Practical Regulation said it in a news release it is joining the Los Angeles County Board of Supervisors, the city of Los Angeles and the Los Angeles Economic Development Corp. in the action against the Los Angeles Regional Water Quality Control Board, which recently adopted the controversial rules. "The cities and the county are absolutely committed to funding common sense programs to improve the quality of water at our local beaches, lakes and rivers," said

Larry Forester, a councilman from Signal Hill and a member of the Coalition's steering committee. "But the Los Angeles board has not conducted any scientific or cost−benefit analyses to justify these regulations. The open−ended nature of the rules leaves cities, and taxpayers, with no financial safety net," he said. **A recent report from the University of Southern California found that the new stormwater rules could lead to the expensive treatment of stormwater, at even greater costs to taxpayers than the region's current wastewater treatment, the coalition said. The USC report found that the construction of stormwater treatment facilities could cost the region between $37 and $326 billion, based on the number of facilities required, the group said.**
Source: http://www.watertechonline.com/news.asp?mode=4font>

[Return to top]

Public Health Sector

Nothing to report.
[Return to top]

Government Sector

17. *January 24, Reuters* — **Tom Ridge sworn in to lead Homeland Security.** Conceived after terrorists killed some 3,000 people on United States' soil on Sept. 11, 2001, the Department of Homeland Security was created to keep Americans safer from terrorist attack. The government's 15th Cabinet−level agency was formed from the merger of 22 federal agencies with 170,000 employees and followed a drawn−out debate on Capitol Hill. **Ridge was sworn at the White House. Bush stood by as Vice President Dick Cheney administered the oath of office. Bush called Ridge "a superb leader who has my confidence."** "We've learned that vast oceans no longer protect us from the dangers of a new era. This government has a responsibility to confront the threat of terrorism where it is found," Bush said in the 10−minute ceremony. Ridge becomes the first secretary of the new Cabinet agency, facing the daunting task of pulling together a massive new agency while defending the nation against terrorism. **Ridge's position is 18th in the line of succession for the presidency, ranking after the Veterans Affairs Department secretary, Anthony Principi. The new department's web site is** http://www.dhs.gov/dhspublic/
Source: http://www.usatoday.com/news/nation/2003−01−24−homeland_x.ht m

18. *January 24, Washington Post* — **Homeland Security Department faces a funding gap for years.** The Department of Homeland Security that formally opened its doors Friday inherits responsibility for a federal government effort that has made little progress in addressing some of the most urgent security vulnerabilities facing American society, terrorism and defense specialists said. From equipping firefighters with protective suits to constructing big−city emergency operations centers to providing U.S. ports with adequate security fences, the street−level demands of protecting U.S. citizens and infrastructure desperately require federal attention, local officials said. **The main problem is money; a politically divided Congress has failed for 11 months to fund some of President Bush's top domestic defense priorities. Budget experts said that federal deficits, as well as the pressing financial needs of U.S.**

military and domestic programs, will keep money for homeland security tight for years. The debate over homeland security spending is being played out on Capitol Hill, with Democrats and a few Republicans pressing for more funds and the Bush administration holding the line on spending. **But even if the advocates of greater spending prevailed, the anti−terrorism effort would still be billions of dollars short each year of the amount many security experts say is needed to harden the United States against attacks.**
Source: http://www.washingtonpost.com/wp−dyn/articles/A35180−2003Jan 23.html

19. *January 24, New York Times* — **Senate blocks privacy project.** The Senate voted today to bar deployment of a Pentagon project to search for terrorists by scanning information in Internet mail and in the commercial databases of health, financial and travel companies here and abroad. **The curbs on the project, called the Total Information Awareness Program, were adopted without debate and by unanimous consent as part of a package of amendments to an omnibus spending bill. House leaders had no immediate comment on the surprise action, which will almost certainly go to a House−Senate conference. Neither did the White House or the Defense Department.** Senator Ron Wyden, the Oregon Democrat who proposed the amendment, said after the vote that it passed so easily because dismayed Republican senators had told him that "this is about the most far−reaching government surveillance proposal we have ever heard about." He said the amendment means "there will be concrete checks on the government's ability to snoop on law−abiding Americans." **Under the legislation passed today, research and development of the system would have to halt within 60 days of enactment of the bill unless the Defense Department submitted a detailed report about the program, including its costs, goals, impact on privacy and civil liberties and prospects for success in stopping terrorists. The research could also continue if President Bush certified to Congress that the report could not be provided or that a halt "would endanger the national security of the United States." The limits on deploying, or using, the system are stricter. While it could be used to support lawful military and foreign intelligence operations, it could not be used in this country until Congress had passed new legislation specifically authorizing its use.**
Source: http://www.nytimes.com/2003/01/24/politics/24PRIV.html

20. *January 23, Government Executive* — **Study says bureaucratic obstacles may hobble Homeland Department.** As Bush administration officials merge more than 22 federal agencies into the Homeland Security Department, complex bureaucratic and organizational challenges could distract them from meeting more urgent counter−terrorism requirements, according to a Brookings Institution report released Thursday entitled "Protecting the American Homeland: One year on." **"The terrorists are not going to wait for us to organize," Ivo Daalder, a Brookings senior fellow in foreign policy studies, said during a briefing on the report. "They're going to strike when they're going to strike, and the challenge ... is to make sure that as we reorganize, we also continue to keep our eye on what is truly important to protect [Americans] against terrorist attacks."** One important requirement is to enhance and integrate many federal, state and local information systems, according to Michael O'Hanlon, a senior fellow in foreign policy studies who co−authored the report with Daalder and five other Brookings scholars. "We need to use information technology much more assertively," O'Hanlon said. "The federal government ... is not spending much money trying to network different agencies together, trying to share information with local law enforcement, trying to get hardware and software compatible." **Constructing that infrastructure requires policymakers**

to "accept the principle that information is going to be shared" between federal entities—such as law enforcement and intelligence agencies—that have a long history of, and cultural resistance to, that type of communication, according to James Steinberg, vice president and director of foreign policy studies. "I think it's a mindset issue," Steinberg said, adding that many federal agencies will have to re−think their classification systems in order to share crucial counterterrorism data with state and local agencies, the private sector, and foreign allies. "It's largely a bureaucratic and organizational problem, and not a technology problem." Homeland security officials also should establish an independent, domestic counter−terrorism agency to collect and analyze information on potential threats, according to the Brookings report. **And it recommended that the Homeland Security Department focus its initial organizational efforts on border and transportation security, protecting critical infrastructures, and improving communications among federal, state and local agencies and the private sector.** The full text of the Brookings study is available at http://www.brook.edu/dybdocroot/views/papers/daalder/2003010 1.pdf
Source: http://www.govexec.com/dailyfed/0103/012303td1.htm

[Return to top]

Emergency Services Sector

Nothing to report.
[Return to top]

Information and Telecommunications Sector

21. *January 26, UPI* — **Massive Internet outage was preventable. A massive Internet outage that swept across Asia and slowed down service in the United States and northern Europe subsided Sunday, caused by a so−called "Slammer" message worm that could easily have been avoided, experts said. Reports of a near universal shutdown of the Internet in South Korea Saturday were accompanied by widespread problems in the United States that shut down some automatic bank teller machine networks, held up e−mail, cut voice−over−Internet service and disrupted many private businesses, including some newspapers.** Hong Kong, South Korea, the northeastern United States and northern Europe appeared to be hit the hardest. Japan and Latin America were the least affected, according to Matrix NetSystems, an Austin, Texas, company that constantly monitors Internet traffic worldwide. "The overall effect of these worldwide performance problems are severe, with more than 30% packet loss globally at the beginning of the event," the company said. "The performance problems seem to be subsiding for the time being" as system operators reacted, either shutting down their servers or installing necessary security fixes. As is typical with malicious worm software, its origin could not be immediately determined. Although the impact varied from region to region, **the outage overall appeared to be the worst for the Internet in at least 18 months. The worm, which unlike a computer virus merely duplicates itself, did its damage by clogging communications from server to server, overloading the capacity of the Internet in many key locations. Although the worm did not spread instructions to harm hard drive storage or trigger other types of secondary damage, it denied or slowed Internet service to untold thousands of users. The effect was a massive "denial of service," a huge overload sometimes purposely directed against single Web sites but this time**

spread worldwide. The worm was dubbed the "Slammer," and exploited a weakness in the widely used Microsoft SQL 2000 server software, a security flaw identified by Microsoft in July of last year. But system operators who had not previously downloaded free repair software since then found the problem suddenly caught up with them Saturday, sometimes in a devastating system stoppage. **"While Web users experienced delays, the underlying Internet was largely unaffected," the company said. "The signature of this event," it continued, "is similar to that of the Goner Worm that struck in December 2001."** Others compared the widespread effect to that of the "Code Red" worm which also afflicted servers running Microsoft software in July of 2001, that time targeting port 80. A patch is available at Microsoft's Web site: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/virus/alerts/slammer.asp.
Source: http://www.upi.com/view.cfm?StoryID=20030126−043023−3604r

22. *January 25, NIPC* — **NIPC Advisory 03−001: "Worm Targets SQL Vulnerability". The NIPC is aware of the propagation of an SQL worm. This exploitation affects users of Microsoft SQL Server 2000, primarily "corporate−level" data base users.** This is not a home user issue unless they are running this server. Starting around 01:30 GMT−0500 on Saturday, January 25, the Internet experienced increased traffic from seemingly random Internet Protocol (IP) source addresses to port 1434/udp targeting a service provided by Microsoft SQL Server. The packets appear to be of a small size (approximately 376 bytes). **Reports indicate that the impact of this activity is causing varied levels of degradation in Internet connectivity.** Early analysis suggests this is a result of scanning from a worm. The worm apparently can easily fill the state table of stateful firewalls, e.g. PIX, Check Point, and Netscreen. **This will cause an outage for the infected site, and the outage may occur long before the data pipes are filled. This issue is also causing problems to routers, both directly and indirectly.** The worm generates some addresses to be attacked, including multicast addresses. This may cause problems for multicast−enabled routers and networks. This worm causes high CPU usage on servers, essentially slowing or shutting servers down. An infected host will spew packets as quickly as the infinite loop will allow. **While an additional malicious "payload" has not yet been identified, this vulnerability essentially exploits a buffer overflow which may allow remote access to a victim's Microsoft SQL data base servers. The NIPC advises users to block or filter port 1434/udp ingress (inbound) and egress (outbound) traffic, and monitor watch port 1433 for any increased traffic load. Microsoft SQL server users are encouraged to review the following web site to ensure they have taken appropriate action to fix that vulnerability:**
http://www.microsoft.com/Downloads/details.aspx?displaylang=en9−B4EB−4446−9BE7−2DE45CFA6A89
Source: http://www.nipc.gov/warnings/advisories/2003/03−001.htm

23. *January 23, Kansas City Channel* — **Hacker downloads information on 1,450 international students.** University of Kansas officials discovered Wednesday that a computer hacker downloaded personal information gathered on 1,450 of its international students. The **information was collected as part of new homeland security measures. The files were for the Student and Exchange Visitor Information System, which will allow universities to transmit information on international students to the Immigration and Naturalization Service (INS) beginning in August. The files included such information as Social Security, passport and university identification numbers, cities and countries of origin and**

programs students were taking. The university alerted INS and FBI officials and said it was told the INS was notifying U.S. ports of entry. **The breach raised concerns someone might use the information to enter the United States illegally**. Marilu Goodyear, the university's vice provost for information services, described the problem as **a "hole" on the computer's security system that could allow a "medium−expert hacker" to break into the computer**. She attributed the problem to Microsoft Windows, not the SEVIS software. "The server was secure when it was installed," she said. "We were installing a security upgrade to the system when a hole we had fixed reverted to its original state."
Source: http://www.thekansascitychannel.com/education/1930636/detail .html

24. *January 23, Wired* — **Security hole discovered in Sprint DSL modems.** Sprint DSL customers are **at risk of having their e−mail addresses and passwords stolen −− even when their computers are powered off −− due to weak security controls on their DSL modems**. Sprint officials acknowledged that **remote access to the administrative software embedded in the ZyXel Prestige 642 and 645 DSL modems is by default protected with a password of "1234**." But the company said users are responsible for securing the equipment, which stores login data, including the user's e−mail address and password. Sprint spokeswoman Laura Tigges admitted that Sprint does not provide instructions for resetting the administrative password in the documentation provided to customers. Not to be confused with the Sprint DSL account password, the administrative password allows a remote user to access the modem's configuration software over the Internet. Sprint could not say how many of its more than 110,000 DSL customers might be affected. Tigges said **Sprint will post instructions on its support website for disabling the remote administration feature, and customers can also get assistance from Sprint's technical support staff. The company also plans to begin shipping DSL modems without the feature beginning in February**, she said.
Source: http://www.wired.com/news/infostructure/0,1377,57342,00.html

Internet Alert Dashboard

Current Alert Levels

AlertCon: 3 out of 4 https://gtoc.iss.net	Security Focus ThreatCon: 3 out of 4 www.securityfocus.com

Current Virus and Port Attacks

Virus:	#1 Virus in the United States: **WORM_KLEZ.H** Source: http://wtc.trendmicro.com/wtc/wmap.html, Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
Top 10 Target Ports	1434 (ms−sql−m), 137 (netbios−ns), 1433 (ms−sql−s), 80 (http), 139 (netbios−ssn), 445 (microsoft−ds), 53 (domain), 4662 (???), 135 (???), 21 (ftp) Source: http://isc.incidents.org/top10.html; Internet Storm Center

[Return to top]

General Sector

25. *January 24, CNN* — **Sixteen arrested in Spain terror raids. Sixteen suspected Islamic terrorists arrested Friday in Spain were "preparing for attacks with explosive and chemical material" in Europe, the Spanish prime minister said.** "The police have arrested 16 activists, dismantling an important network linked to al Qaeda and the Algerian Salafist group," Prime Minister Jose Maria Aznar said during a nationally televised news conference. **A government statement said the 16, mainly Algerians, were preparing to send communications gear to Chechnya and Algeria and had been trying to obtain a private broadcasting hookup that could extend 3,000 kilometers (1,860 miles). Police on Friday found chemical material that included "hydrocarbons and synthetic material." The material is being analyzed by police**, said Interior Minister Angel Acebes. Authorities also seized electronic gear that could be used in attacks, such as remote control devices that could set off bombs. "The suspects provided information and infrastructure to other Islamic terrorist groups, and they had explosives, used chemical products and had connections to other terrorist cells in the United Kingdom and France," the government statement said.
Source: http://www.cnn.com/2003/WORLD/europe/01/24/spain.us.intellig ence/

26. *January 24, Guardian Unlimited* — **Italy terror suspects had maps of London. Italian police were questioning five Moroccan men today about a possible terrorist plot to attack London and NATO bases in Italy, after a routine immigration sweep uncovered explosives.** The five Moroccan men were arrested on Wednesday at an abandoned farmhouse outside of Rovigo, a town in northern Italy about 30 miles south−west of Venice. **Police who had been looking for illegal immigrants discovered a kilo of explosives, believed to be C4, and maps of central London. Police also reportedly found maps marking the site of Italian churches and NATO bases.** Police sources in Italy were reported to believe that the men had been in contact with terrorist cells in Britain. Reports suggested police had found several Arabic documents which were addressed to or had been sent from the UK.
Source: http://www.guardian.co.uk/international/story/0,3604,881649, 00.html

27. *January 24, CNN* — **Sources: Senior al Qaeda official may have been in Iraq.** A senior al Qaeda leader may provide a link between that terrorist group and Iraq, according to coalition intelligence sources. **Abu Mussab al Zarqawi −− a Jordanian −− was recently accused by Jordanian officials of masterminding the assassination of U.S. diplomat Laurence Foley in Amman in late October. And Zarqawi has been linked to some of the men arrested recently in London and accused of possessing the deadly poison ricin.** But it is his travels, especially in the past year, that have attracted the attention of intelligence officials. **Zarqawi, coalition intelligence sources said, left Afghanistan when the Taliban regime was toppled. From there, said the sources, he traveled through Iran to Baghdad, then to Kurdish−controlled areas of northern Iraq, where Ansar al−Islam, a group linked to al Qaeda, operates.** Some in the U.S. intelligence community have questioned whether officials in these countries were aware of Zarqawi's presence, because he might have been using aliases. But former CIA operative Robert Baer, who spent years in the Middle East, disagreed. **"Somebody at some level had to know he was there. Now obviously I can't tell you whether Saddam knew, but somebody in an official line of responsibility for customs and**

immigration knew he came into the country," Baer said. "Palestinians, other Arabs, even Iraqis go through a very tight screen when they come into that country. Documents are looked at. You just can't do it [sneak in]. It is a police state." Coalition intelligence sources say Zarqawi also traveled to Syria and Lebanon, moving with seeming ease between those countries, setting up terrorist cells. These sources say Zarqawi is believed now to be in Iran. Source: http://www.cnn.com/2003/WORLD/meast/01/23/iraq.alqaeda/index .html

[Return to top]

NIPC Products &Contact Information

The National Infrastructure Protection Center (NIPC) serves as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity. The NIPC provides timely warnings of international threats, comprehensive analysis and law enforcement investigation and response. The NIPC provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the NIPC web−site (http://www.nipc.gov), one can quickly access any of the following NIPC products:

NIPC Advisories − Advisories address significant threat or incident information that suggests a change in readiness posture, protective options and/or response.

NIPC Alerts − Alerts address major threat or incident information addressing imminent or in−progress attacks targeting specific national networks or critical infrastructures.

NIPC Information Bulletins − Information Bulletins communicate issues that pertain to the critical national infrastructure and are for informational purposes only.

NIPC CyberNotes − CyberNotes is published to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure−related best practices.

NIPC Daily Open Source Report Contact Information

Content and Suggestions:	Melissa Conaty (202−324−0354 or mconaty@fbi.gov) Kerry J. Butterfield (202−324−1131 or kbutterf@mitre.org)
Distribution Information	NIPC Watch and Warning Unit (202−323−3204 or nipc.watch@fbi.gov)

NIPC Disclaimer

The NIPC Daily Open Source Report is a daily [Monday through Friday] summary and assessment of open−source published information concerning significant critical infrastructure issues. This is an internal NIPC tool intended to serve the informational needs of NIPC personnel and other interested staff. Further reproduction or redistribution for private use or gain is subject to original copyright restrictions of the content. The NIPC provides no warranty of ownership of the copyright, or of accuracy in respect of the original source material.